UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/827,291	04/05/2001	Colin A. Waters	9385	5721

26884 7590 10/08/2004

PAUL W. MARTIN
LAW DEPARTMENT, WHQ-4
1700 S. PATTERSON BLVD.
DAYTON, OH 45479-0001

EXAMINER	
ABDI, KAMBIZ	

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 10/08/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/827,291	Applicant(s) WATERS ET AL.
	Examiner Kambiz Abdi	Art Unit 3621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 April 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 April 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 2.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-14 have been examined and are pending.

Drawings

2. The formal drawings were received on 12 October 2001 and they have been entered as paper number 3.

Claim Objections

3. Claims 2 and 4 are objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. Both claims essentially repeat the same limitation "payment device generates a digital signature from said captured biometric data".

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 3, 8-11, 13, and 14 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,202,151 to Clyde Musgrave et al.

6. As per claim 3, Musgrave discloses a system for supporting consumer access to a financial account by means of biometric data solely comprising:

a biometric data capture device for capturing biometric data corresponding to a consumer (See Musgrave figure 3 where the biometric data of first user that corresponds to the applicant's consumer are captured at element 26, column 4, lines 23-30); and

a payment device for sending said captured biometric data (See Musgrave column 6, lines 5-18 and column 4, lines 57-65, where the receiver 44, corresponds to applicant's merchant payment host, transfers funds where the transferring of funds corresponds to applicant's payment upon authentication) to a merchant payment host as the identifier for the consumer's financial account data (See Musgrave column 6, lines 16-18, discloses that upon authenticity an electronic transaction is processed. Column 6, lines 42-52, discloses the biometric data incorporated within the transmission message does contain instructions to lookup bank account data and other financial information in order to authenticate a transaction).

7. As per claim 8, Musgrave discloses a method for authorizing access to a financial account for a consumer comprising:

generating a data storage key from biometric data (biometric certificate) corresponding to a consumer (See Musgrave abstract, figure 1-3, column 5, lines 44-59); and

retrieving a data record corresponding to the generated data storage key, the data record containing financial account data for the consumer (See Musgrave column 6, lines 16-18 and lines 42-52).

8. As per claim 9, Musgrave discloses the method of claim 8 further comprising:

generating a digital signature from the biometric data (See Musgrave column 5, lines 29-32, where generating a digital signature incorporating biometric data is disclosed) corresponding to the consumer to authorize generation of electronic funds transfer messages for a financial transaction (See Musgrave column 5, lines 32-36, where transmission over a network of digital signature is a transaction message, also column 6, lines 12-18 and column 4, lines 57-65, where the receiver 44, corresponds to applicant's merchant payment host, transfers funds where the transferring of funds corresponds to applicant's payment upon authentication).

9. As per claim 10, Musgrave discloses the method of claim 8 further comprising:

capturing the biometric data corresponding to the consumer (See Musgrave column 6, lines 5-18 and column 4, lines 57-65, where the receiver 44, corresponds to applicant's merchant payment host, transfers funds where the transferring of funds corresponds to applicant's payment upon authentication); and

transmitting the captured biometric data so the data storage key may be generated (See Musgrave column 6, lines 5-18 and column 4, lines 57-65, where the receiver 44, corresponds to applicant's merchant payment host, transfers funds where the transferring of funds corresponds to applicant's payment upon authentication).

10. As per claim 11, Musgrave discloses the method of claim 9 further comprising:

comparing the generated digital signature to a received digital signature to authorize generation of electronic funds in response to said generated digital signature corresponding to said received digital signature (See Musgrave column 5, lines 29-36, where it discloses the generation of digital signature; column 5, lines 60-63 discloses a comparator for comparison of digital data (digital signature, biometric data, has value and other recorded data); column 6, lines 12-18 and column 4, lines 57-65, where the receiver 44, corresponds to applicant's merchant payment host, transfers funds where the transferring of funds corresponds to applicant's payment upon authentication and where digital signature is appended to the transaction data(electronic finds transfer).

11. As per claim 13, Musgrave discloses a method for accessing a financial account of a consumer comprising:

capturing biometric data corresponding to a consumer (See Musgrave figure 3 where the biometric data of first user that corresponds to the applicant's consumer are captured at element 26, column 4, lines 23-30); and

sending the captured biometric data to a merchant payment host (See Musgrave column 6, lines 5-18 and column 4, lines 57-65, where the receiver 44, corresponds to applicant's merchant payment host, transfers funds where the transferring of funds corresponds to applicant's payment upon authentication) to obtain financial account data from the merchant payment host (See Musgrave column 6, lines 16-18, discloses that upon authenticity an electronic transaction is processed. Column 6, lines 42-52, discloses the biometric data incorporated within the transmission message does include bank account data and other financial information).

12. As per claim 14, Musgrave discloses method of claim 13 further comprising:

generating a digital signature from the captured biometric data (See Musgrave column 5, lines 29-32, where generating a digital signature incorporating biometric data is disclosed); and transmitting the generated signature in a transaction message (See Musgrave column 5, lines 32-36, where transmission over a network of digital signature is a transaction message) to the merchant payment host for authorizing generation of electronic transfer messages by the merchant payment host (See Musgrave column 6, lines 12-18 and column 4, lines 57-65, where the receiver 44, corresponds to applicant's merchant payment host, transfers funds where the transferring of funds corresponds to applicant's payment upon authentication).

Claim Rejections - 35 USC § 103

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

14. Claims 1, 2, 4, 6, 7, and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,202,151 to Clyde Musgrave et al. in view of U.S. Patent No. 6,618,806 to Timothy j. Brown et al.

15. As per claim 1, Musgrave discloses a system for providing consumer access to a financial account to implement a transaction comprising:

Musgrave discloses a biometric data capture device for reading consumer biometric data (See Musgrave figure 3 where the biometric data of first user that corresponds to the applicant's consumer are captured at element 26, column 4, lines 23-30); and

What Musgrave is not explicit on is, a database server for generating a data storage key from the consumer biometric data received from the biometric data capture device and for retrieving a data record corresponding to the generated data storage key.

However, Brown clearly discloses that a biometric identifier record (BIR) (data storage key) is created in relation to the biometric data captured at the capture device (See Brown column 2, lines 19-26, column 4, lines 1-15) and stored in order to be utilized as an identifier of the records (biometrics data, financial, personal, etc.) kept in a database in relation to such identifier (See Brown column 4, lines 42-47).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the current invention was made to use the teachings of the Musgrave in conjunction with that of Brown for the motivation of better efficiency and accuracy of looking up information in relation to biometric data identification and authentication.

16. As per claims 2 and 4, Musgrave discloses the system of claim 1 further comprising:

a payment device coupled to said biometric data capture device (See Musgrave figure 3 and 4 and column 4, lines 53-59, where transaction data input device 30 corresponds to payment device, which is corresponding to an electronic funds transfer), said payment device generating a digital signature from said biometric data for a transaction message (See Musgrave column 5, lines 29-32, where generating a digital signature incorporating biometric data is disclosed).

17. As per claim 6, Musgrave discloses a system for verifying access to a consumer's financial account comprising:

Musgrave discloses generating a data storage key (biometric certificate) from biometric data received from a transaction site (See Musgrave abstract, column 5, lines 44-59); and

Also Musgrave discloses an identity database (biometric database) comprised of data records stored with reference to a data storage key corresponding to biometric data contained within the data record (biometric database) so that the database server may retrieve records from the identity database using data storage keys generated from the received biometric data (See Musgrave abstract, figure 4 and column 3, lines 40-63, column 5, lines 46-59).

What Mugrave is not explicit on is a database server for generating a data storage key.

However, Brown clearly discloses that a biometric identifier record (data storage key) is created in relation to the biometric data captured at the capture device (See Brown column 2, lines 19-26, column 4, lines 1-15) and stored in order to be utilized as an identifier of the records (biometrics data, financial, personal, etc.) kept in a database in relation to such identifier (See Brown column 4, lines 42-47).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the current invention was made to use the teachings of the Musgrave in conjunction with that of Brown for the motivation of better efficiency of looking up information in relation to identification and authentication.

18. As per claim 7, Musgrave discloses the system of claim 6 wherein the database server generates a digital signature from biometric data retrieved from the identity database so that a transaction message may be verified (See Musgrave column 3, lines 40-57 and column 5, lines 29-32, where generating a digital signature incorporating biometric data is disclosed).

19. As per claim 12, Musgrave discloses the method of claim 8 wherein the generated key corresponds to name data and the retrieval includes:

Musgrave discloses comparing the biometric data stored in the retrieved data records to other biometric data received from a merchant purchase site (See Musgrave column 5, lines 29-36, where it discloses the generation of digital signature where the digital signature includes biometric data; column 5, lines 60-63 discloses a comparator for comparison of digital data (digital signature, biometric data, has value and other recorded data).

What Musgrave does not explicitly disclose is retrieving a plurality of data records corresponding to the generated key.

However, Brown clearly discloses that a biometric identifier record (data storage key) is created in relation to the biometric data captured at the capture device (See Brown column 2, lines 19-26, column 4, lines 1-15) and stored in order to be utilized as an identifier of the records (biometrics data, financial, personal, etc.) kept in a database in relation to such identifier (See Brown column 4, lines 42-47).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the current invention was made to use the teachings of the Musgrave in conjunction with that of Brown for the motivation of better efficiency of looking up information in relation to identification and authentication.

Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,202,151 to Clyde Musgrave et al. and of U.S. Patent No. 6,618,806 to Timothy j. Brown et al. further in view of U.S. Patent no. 5,493,621 to Yoshihide Matsumura.

20. As per claims 5, Musgrave and Brown disclose the system of claims 1; further,

Musgrave and Brown disclose the generated key is name data and the database server retrieves a data records corresponding to the generated key (See Brown column 2, lines 19-26, column 4, lines 1-15) and

determines whether biometric data stored in any of the retrieved data records corresponds to a biometric data received from a merchant purchase site (See Brown column 4, lines 42-47).

What Musgrave and Brown are not explicit on is the plurality of the records corresponding to the same key (BIR) (See Brown column 2, lines 19-26, column 4, lines 1-15).

However, Matsumura clearly discloses that an identifier (ID number, here BIR) can be used to narrow the field of search within the vast number of finger print data stored for registered users (See Matsumura column 11, lines 44-54). It is clear that using the ID number as an index key to locate a finger print data substantially speeds up the time required as well as the accuracy of the matching. Additionally, Matsumura clearly discloses that this index key (BIR) could be related to a plurality of persons (plurality of data records corresponding to generated key) registered with the system.

Therefore, it would have been obvious to one having ordinary skill in the art at the time the current invention was made to use the teachings of the Musgrave in conjunction with that of Brown and further in combination with Matsumura for the motivation of substantially reducing the number of data to be search as well as time and speeding up the search in a data storage that is required, and the accuracy of the matching of finger prints data.

21. Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

Conclusion

22. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kambiz Abdi whose telephone number is (703) 305-3364. The examiner can normally be reached on 9 AM to 5:00 PM.

23. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James P Trammell can be reached on (703) 305-9768. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

24. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

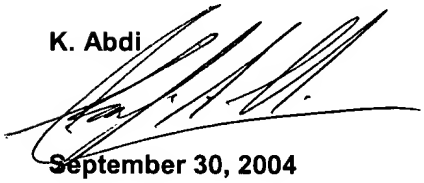
Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
Washington D.C. 20231

Hand delivered responses should be brought to:

Crystal Park 5, 2451 Crystal Drive
7th floor receptionist, Arlington, VA, 22202

K. Abdi



September 30, 2004